DRN: ____________________

SUBSCRIPTION OF MANAGED SERVICES FOR DSWD COMPLETE SUITE OF PRIMARY ICT SECURITY DEVICES

(ITB No. GOP/20-DSWD-017)

03 JANUARY 2020 | 03:00 PM

OUS-DRMG Conference Room, Directors Dormitory, DSWD Central Office

MINUTES OF PRE-BID CONFERENCE

I. Attendance

Bids and Awards Committee (BAC):

1. U/Sec. Felicisimo C. Budiongan	-	Chairperson
2. U/Sec. Rene Glen O. Paje	-	Regular Member
3. Dir. Andrew J. Ambubuyog	-	Provisional Member

BAC Secretariat:

1. Ms. Oliva C. Arcaina	-	Supervising Administrative Officer
2. Mr. William V. Garcia Jr.	-	Administrative Officer V
3. Mr. Ramon M. Villareal Jr.	-	Administrative Officer V
4. Mr. Patrick Glenn A. Leynes	-	Administrative Officer IV
5. Mr. Ramises B. Esteban	-	Administrative Officer III
6. Mr. Lourence C. Buenaventura	-	Administrative Officer II
7. Ms. Danilyn A. Dedeles	-	Administrative Assistant III
8. Ms. Marden D. Aquino	-	Administrative Assistant III

Others in Attendance:

1. Mr. Sandy Roy L. Ocampo	-	Information and Communications Technology Management Service (ICTMS)
2. Mr. Jeson M. Diaz	-	ICTMS
3. Mr. Joshua Kevin J. Jovellanos	-	Procurement Management Service (PMS)–Contract Monitoring Division (CMD)

Prospective Bidder/s Present:

1. Mr. Chris Garcia	-	Accent Micro Technologies, Inc.
2. Mr. Ryelan Bautista	-	Accent Micro Technologies, Inc.

II. Call to Order

The Pre-Bid Conference for the **"Subscription of Managed Services for DSWD Complete Suite of Primary ICT Security Devices"** was called to order at **03:00 PM** by the BAC Chairperson, **U/Sec. Felicisimo C. Budiongan**. He then introduced the members of the BAC, the BAC Secretariat and the representatives from the End-user (Information and Communications Technology Management Service) and Procurement Management Service. *(Note: The other invited observers were unable to attend.)* He also acknowledged the presence of representatives of the prospective bidder.

A copy of the Agenda is hereto attached, marked as **Annex "A"**, and made an integral part hereof.

III. Highlights of Discussion

ITEM/ PARTICULAR	ISSUES/ CONCERNS / DISCUSSIONS	AGREEMENTS/ ACTION REQUIRED
Procurement Guidelines	• Ms. Arcaina *(BACSec)* presented the procurement guidelines for the information of the prospective bidder.	
Background of the Project	• Mr. Ocampo *(ICTMS)* provided the background of the project. He mentioned that the project aims to subscribe to a comprehensive, expertly managed, and maintained the primary security devices which will be readily available for DSWD including their pool of expert personnel for managing, maintenance, troubleshooting and repair services.	
Schedule of Requirements - Payment Schedule	• Mr. Garcia *(Accent Micro)* asked for the payment schedule. • Mr. Ocampo *(ICTMS)* replied that the payment scheme based on the deliverables, hence, shall be done per completion of milestones. • Mr. Jovellanos *(PMS–CMD)* observed that the billing of services is quarterly. • Mr. Ocampo *(ICTMS)* corrected the provision. He stated the billing should be issued every after deliverables. • Ms. Arcaina *(BACSec)* stated that a supplemental/ bid bulletin shall be issued for the correction.	

Preparation of Bid Proposals	• Ms. Arcaina *(BACSec)* reminded the prospective bidder on how to prepare bid proposal and how to accomplish the forms in the Bidding Documents.	
Deadline of Submission and Reciept of Queries and Clarifications	• Mr. Garcia Jr. *(BACSec)* reminded the prospective bidder that queries and clarifications may be submitted to the BAC Secretariat on or before 06 January 2020, 05:00 PM, in writing or thru email at bacsec@dswd.gov.ph or thru fax at (02) 951-7116.	

IV. Adjournment

Having no other matters for discussion, the Pre-Bid Conference was adjourned at **03:30 PM**.

Prepared by:

DANILYN A. DEDELES
Administrative Assistant III
Bids and Awards Committee Secretariat

Noted by:

OLIVA C. ARCAINA
Supervising Administrative Officer and Officer-in-Charge, Bids and Awards Committee Secretariat

Approved by:

FELICISIMO C. BUDIONGAN
Undersecretary and
Chairperson, Bids and Awards Committee

PRE-BID CONFERENCE

DESCRIPTION	:	Subscription of Managed Services for DSWD Complete Suite of Primary ICT Security Devices | ITB No. GOP/20-DSWD-017
DATE	:	03 January 2020
TIME	:	03:00 PM
VENUE	:	OUS-DRMG Conference Room, Room 202, Directors Dormitory
PARTICIPANTS	:	*BAC, BAC Secretariat, ICTMS, FMS, PMS, Prospective Bidders*

AGENDA

I. Call to Order

A. Introduce the members of the BAC, the BAC Secretariat, and other DSWD Personnel present.

B. Acknowledge the presence of all interested bidders who are in attendance.

C. Inform the bidders that questions will be entertained after the reading of the Rules Specified in the Bidding Documents.

II. Procurement Guidelines

A. The procurement procedure for the **"Subscription of Managed Services for DSWD Complete Suite of Primary ICT Security Devices"** is Competitive Bidding pursuant to the provisions of Republic Act No. 9184 (RA 9184) and its revised 2016 Implementing Rules and Regulations (IRR), otherwise known as the "Government Procurement Reform Act" (GPRA).

B. All bids will be opened, read aloud, and recorded at the time of the bid opening. **Late bids will be marked "Late" and will be returned unopened to the bidder.** No award shall be made during the bid opening. During the bid opening, the Bids and Awards Committee (BAC) will conduct a preliminary examination of the bid proposals submitted to determine its completeness, check if the required bid security has been posted, and that the documents have been properly signed and are generally in order.

C. Deviations

Bidders are not allowed to deviate from any of the eligibility, technical and financial specifications specified in the bidding documents. Bids exhibiting non-compliance with the specifications shall be disqualified.

D. Evaluation and Comparison of Bids

The Procuring Entity will evaluate and compare bids, which have been determined to be responsive during the preliminary examination.

III. The Bidding Documents shall be discussed by the Head of the BAC Secretariat, particularly the following issues:

A. Eligibility and Technical Component

All the required Eligibility and Technical Documents listed on the Instructions to Bidders (ITB) and the Bid Data Sheet (BDS) shall be submitted following such order. Those documents shall be the basis of the preliminary examination of bids.

B. Financial Component

All the required Financial Documents listed in the ITB and BDS shall be submitted, following such order. Those documents will be the basis of the Preliminary Examination of the Financial Proposal during the bid opening.

C. Preliminary Examination

The BAC shall open the **Eligibility and Technical Component (first envelope)** and check the submitted eligibility and technical documents for each bidder against a checklist of required eligibility and technical documents to ascertain if they are all present, **using non-discretionary "pass/fail" criteria**. In case one or more of the required documents is missing, the BAC shall declare the eligibility and technical requirement concerned as **"failed"** and immediately return to the bidder concerned its Financial Component (second envelope). Otherwise, the BAC shall declare the said eligibility requirements as **"passed"**.

Upon completion of the preliminary examination of the Eligibility and Technical component, the BAC shall subsequently open the **Financial Component (second envelope)** and check against a checklist of required financial documents to ascertain if they are all present **using a non-discretionary "pass/fail" criteria**. In case one or more of the financial documents required are missing and/or if the submitted total bid price exceeds the Approved Budget for the Contract (ABC), the BAC shall declare the bid concerned as **"failed"**.

D. Bid Security

Each bidder shall furnish a Bid Security as part of its Bid. The Bid Security shall be in any of the form prescribed on the ITB.

E. Bid Validity Period

Bids shall be valid for **one hundred twenty (120) calendar days** from the date of the opening of bids.

F. Evaluation and Award

The BAC or the designated Technical Working Group (TWG) will conduct a detailed evaluation and comparison of all bids declared "passed", using non-discretionary criteria. Those who complied with the criteria prescribed in the bidding documents will be ranked in ascending order of their total calculated bid prices, as evaluated and corrected for computational errors, discounts and other modifications to determine the Lowest Calculated Bid (LCB).

G. Post-Qualification

After determining the **Lowest Calculated Bid (LCB)** or **Single Calculated Bid (SCB)**, as the case maybe, the BAC shall conduct post-qualification to verify, validate, and ascertain all statements made and documents submitted by the bidder with the LCB/SCB, using non-discretionary criteria. If the BAC determines that the bidder with the LCB/SCB passes all the criteria for post-qualification, it shall declare the said bidder as the **Lowest Calculated and Responsive Bid (LCRB)** or **Single Calculated and Responsive Bid (SCRB)** and award the contract to the said bidder.

IV. Open Forum

Any clarifications, issues or concerns that are not found in the bid documents will be announced in writing through Supplemental/Bid Bulletin.

V. Adjournment

DSWD
Department of Social Welfare and Development

INVITATION TO BID FOR

SUBSCRIPTION OF MANAGED SERVICES FOR DSWD COMPLETE SUITE OF PRIMARY ICT SECURITY DEVICES

— ITB No. GOP/20-DSWD-017 —
(PR No. 2019121827)

1. The **Department of Social Welfare and Development (DSWD)**, through the **DSWD** Funds, intends to apply the sum of **Thirty-Eight Million Pesos (PHP 38,000,000.00)**, being the Approved Budget for the Contract (ABC) to payments under the contract for the **Subscription of Managed Services for DSWD Complete Suite of Primary ICT Security Devices.** Bids received in excess of the ABC shall be automatically rejected at bid opening.

2. The DSWD now invites registered Philippine Government Electronic Procurement System (PhilGEPS) service providers to bid for the **Subscription of Managed Services for DSWD Complete Suite of Primary ICT Security Devices.** Delivery of Goods and Services shall be in accordance with **Section VI. Schedule of Requirements.** Bidders should have completed, **within five (5) years from the date of submission and receipt of bids**, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II. Instructions to Bidders.

3. Bidding will be conducted through open competitive bidding procedures using a non-discretionary “pass/fail” criterion as specified in the 2016 Revised Implementing Rules and Regulations (IRR) of Republic Act (RA) 9184, otherwise known as the “Government Procurement Reform Act”.

   Bidding is restricted to Filipino citizens/sole proprietorships, partnerships, or organizations with at least sixty percent (60%) interest or outstanding capital stock belonging to citizens of the Philippines, and to citizens or organizations of a country the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to RA 5183.

4. Interested bidders may obtain further information from **DSWD Bids and Awards Committee (BAC) Secretariat** and inspect the Bidding Documents at the address given below from **Monday** to **Friday** at ***08:00 AM*** to ***05:00 PM.***

5. A complete set of Bidding Documents may be purchased by interested Bidders on ***27 December 2019*** to ***15 January 2020*** from the address below and upon payment of a nonrefundable fee for the Bidding Documents in the amount of **Twenty-Five Thousand Pesos (PHP 25,000.00).**

   It may also be downloaded free of charge from the website of the PhilGEPS and the website of the Procuring Entity, provided that Bidders shall pay the nonrefundable fee for the Bidding Documents not later than the submission of their bids.

6. The DSWD will hold a **Pre-Bid Conference** on ***03 January 2020, 03:00 PM,*** at the **Office of the Undersecretary for Disaster Response Management Group (OUS-DRMG) Conference Room, Room 202, Directors Dormitory, DSWD Central Office, IBP Road, Constitution Hills, Quezon City** which shall be open to all interested parties.

7. Bids must be delivered to the address below on or before ***15 January 2020, 09:00 AM.*** All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in **ITB** Clause 18.

   Bid opening shall be on ***15 January 2019, 03:00 PM,*** at the **Office of the Undersecretary for Disaster Response Management Group (OUS-DRMG) Conference Room, Room 202, Directors Dormitory, DSWD Central Office, IBP Road, Constitution Hills, Quezon City**. Bids will be opened in the presence of the Bidders' representatives who choose to attend. Late bids shall not be accepted.

8. To facilitate the immediate implementation of the procurement of this Project, the DSWD shall proceed with the conduct of Early Procurement Activities (EPA), pursuant to Section 7.6 (as amended[1]) of the 2016 Revised IRR of RA 9184, Section 19 of the General Provisions of the FY 2020 National Expenditure Program (NEP) and Government Procurement Policy Board (GPPB) Resolution No. 14-2019 dated 17 July 2019.

9. The DSWD reserves the right to reject any and all bids, declare a failure of bidding, or not award the contract at any time prior to contract award in accordance with Section 41 of RA 9184 and its 2016 Revised IRR, without thereby incurring any liability to the affected bidder or bidders.

10. For further information, please refer to:

    THE CHAIRPERSON
    DSWD Bids and Awards Committee
    c/o BAC Secretariat
    Ground Floor, DSWD Central Office
    IBP Road, Constitution Hills, Quezon City
    Fax No. (02) 931-6139
    Telephone Nos. (02) 931-8101 to 07 Local 122 or 124

FELICISIMO C. BUDIONGAN
Undersecretary and
Chairperson, Bids and Awards Committee

[1] GPPB Resolution No. 14-2019 dated 17 July 2019

Section VI. Schedule of Requirements

Subscription of Managed Services for DSWD Complete Suite of Primary ICT Security Devices

Particulars	Quantity
A. Central Office	
• 10G Next Generation Firewall for CO Wide Area Network (WAN)	• 2 Units (HA mode)
• Next Generation Firewall for Local Area Network (LAN)	• 2 Units (HA mode)
• 10G Next Generation IPS for CO (upgraded capacity)	• 2 Units (1 sensor, 1 Management Console)
• FWCentralize Management	• 1 Unit (Admin Management for all Firewall)
B. Field Offices	
• Next Generation Firewall for FOs	• 17 Units (16 FOs, 1 spare)
C. Disaster Recovery Site	
• Next Generation Firewall for DR	• 2 Units (HA mode)
• 10G Next Generation IPS for DR	• 1 Sensor Unit

Delivery Sites:

1. Central Office – DSWD Complex, Batasan Hills, Quezon City
2. Disaster Recovery Site – Clark Pampanga (whichever is the active DR Site of DSWD for the year)
3. 16 Field Offices
   a. DSWD Field Office 1 – San Fernando City, La Union
   b. DSWD Field Office 2 – Carig, Sur, Tuguegarao City
   c. DSWD Field Office 3 – San Fernando City, Pampanga
   d. DSWD Field Office 4A – Muntinlupa City
   e. DSWD Field Office 4B – Malate, Manila
   f. DSWD Field Office 5 – Legaspi City, Albay
   g. DSWD Field Office 6 – Molo, Iloilo
   h. DSWD Field Office 7 – Cebu
   i. DSWD Field Office 8 – Tacloban City, Leyte
   j. DSWD Field Office 9 – Zamboanga,Del Sur
   k. DSWD Field Office 10 – Misamis Oriental, CDO
   l. DSWD Field Office 11 – Davao Del Sur
   m. DSWD Field Office 12 – Koronadal City, South Cotabato
   n. DSWD Field Office CARAGA – Butuan City, Agusan Del Norte
   o. DSWD Field Office CAR – Baguio City, Benguet
   p. DSWD Field Office NCR – Legarda, Manila

Coverage:

- Implementation: Sixty (60) working days for all components
- Maintenance and Support Coverage: until 31 December 2019

Payment Schedule:

Con	Project Phases	Expected Deliverables	Completion Indicators	Payment (% of Total Contract Price)
1	Kick-off and Inception (10 working days after NTP)	• Kick-off documentation and Inception Report • Approved Implementation Plan	• Submitted Kick-off documents and both Party Agreements • Submitted Inception Reports • Submitted and Approved Implementation Plan	10%
2	Supply and Delivery of Firewall Devices and IPS Devices (40% working days after NTP)	• Delivery of Firewall and IPS equipment to all locations • Acceptance Report	• Complete Delivery Receipts	40%
3	Configuration, Testing and Acceptance (60% working days after NTP)	• Setup and Configuration • Successful Testing and Turn-over	• Complete Documentation • User's Acceptance	25%
4	Management, Monitoring and Maintenance Support Checkpoint (180 days after NTP)	• Consolidation of Monthly Operation Report • Training Vouchers or Training Certificate • Summary of Interventions and issue resolutions provided	• Certificate of Satisfactory Service Completion	25%

Issuance of billing will come after each quarter. Payment processing will take **fifteen (15) working days** upon receipt of Sales Invoice or Billing Statement with complete supporting documents.

Name of Bidder: ____

Name of Authorized Representative: ______________________________

Signature of Authorized Representative: __________________________

Date: ____________________

Technical Specifications

DSWD Specifications	Bidder's Specifications[7]
I. NEXT GENERATION UNIFIED THREAT MANAGEMENT **A. CENTRAL OFFICE (CO) REQUIREMENT** **1. Next Generation Unified Threat Management for Wide Area Network** 1.1. Functional Requirements *Platform* 1.1.1. The Service Provider shall propose two (2) 10G Next Generation Firewalls with a capability of supporting at least fifteen (15) gigabit per second of application firewall throughput and at least eight (8) gigabit per second for threat prevention and modern malware protection. 1.1.2. The proposed firewalls shall support at least three (3) million concurrent sessions and at least ONE HUNDRED AND FIFTU THOUSAND (150,000) new sessions per second. 1.1.3. The proposed firewalls shall support at least FIVE THOUSAND (5,000) concurrent sessions of SSL VPN clients inclusive of any required subscription licenses. 1.1.4. The proposed firewalls should have at least TWENTY (20) 10G network ports inclusive of at least twenty (20) SPF+	Brand: Detailed Specifications:

[7] *IMPORTANT NOTE: Detailed specifications must be provided. Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidders statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the provisions of* ***ITB*** *Clause 3.1(a)(ii) and/or* ***GCC*** *Clause 2.1(a)(ii).*

transceivers.

1.1.5. The proposed firewalls must allow policy rule creation for application identification, user identification, threat prevention, Uniform Resource Locator (URL) filtering, traffic management Quality of Service (QoS) per policy and scheduling in a single unified rule and not in multiple data-entry locations in the management console.

1.1.6. The proposed firewalls shall have the hardened Operating System (OS) and built as a firewall appliance (i.e. not on generic server hardware) and shall handle traffic in a stream-based manner with all features turned on. It shall be optimized for layer 7 application level content processing and have special Application-Specific Integrated Circuit (ASIC) to handle signature matching and processing in a single pass parallel processing architecture.

1.1.7. The proposed firewalls shall be administered centrally by the same brand use for central management of all the firewalls to ensure full compatibility and optimized configuration.

1.1.8. The proposed firewall shall have modern malware protection that identifies unknown malicious files by directly and automatically executing them in a virtual cloud-based environment to expose malicious behavior even if the malware has never been seen in the wild before without the need for additional hardware;

1.1.9. Proposed firewall must be configured with **HIGH AVAILABILITY.**

1.1.10. The proposed firewalls must have passed and been certified by third party evaluations (e.g. NSS Labs, ICSA Labs, CSfC, ANSSI).

1.2. Please see additional feature specifications on **ANNEX "A".**

2. Next Generation Unified Threat Management for CO Local Area Network

2.1. Functional Requirement

Platform

2.1.1. The Service Provider shall propose two (2) Next Generation Firewall (inclusive of 1 spare) with a capability of supporting at least FIVE (5) gigabit per second of application firewall throughput and TWO (2) gigabit per second for threat prevention and modern malware protection.

2.1.2. The proposed firewalls shall support at least ONE (1) million concurrent sessions and at least ONE HUNDRED AND TWENTY THOUSAND (120,000) new sessions per second.

2.1.3. The proposed firewalls must allow policy rule creation for application identification, user identification, threat prevention, Uniform Resource Locator (URL) filtering, traffic management Quality of Service (QoS) per policy and scheduling in a single unified rule and not in multiple data-entry locations in the management console.

2.1.4. The proposed firewalls shall have the hardened Operating System (OS) and built as a firewall appliance (i.e. not on generic server hardware) and shall handle traffic in a single pass stream-based manner with all features turned on. It shall be optimized for layer 7 application level content processing and have special Application-Specific Integrated Circuit (ASIC) to handle signature matching and processing in a single pass parallel processing architecture.

2.1.5. The proposed firewalls shall be administered centrally by the same brand use for central management of all the firewalls.

2.1.6. The proposed firewall shall have modern malware protection that identifies unknown malicious files by directly and automatically executing them in a virtual cloud-based environment to expose malicious behavior even if the malware has never been seen in the wild before without the need for additional hardware.

2.1.7. Proposed firewall must be configured with HIGH AVAILABILITY.

2.1.8. The proposed firewalls must have passed and been certified by third party evaluations (e.g. NSS Labs, ICSA Labs, CSfC, ANSSI).

2.2. Please see additional feature specifications on **ANNEX "A".**

3. Next Generation Firewall Centralize Management Platform for CO

3.1. Feature Specifications

Platform

3.1.1. The Service Provider shall propose ONE (1) Next Generation Firewall Centralized Management Appliance with a capability of supporting at least TWENTY FIVE (25) remote firewall.

3.1.2. The proposed Centralized Firewall Management must be capable of both PASSIVE and ACTIVE high availability setup.

3.1.3. The proposed Centralized Firewall Management must be capable of both Local and RADIUS administrator's authentication.

3.1.4. The proposed Centralized Firewall Management must have GUI, Command Line Interface XML-Based REST API for management console.

3.1.5. The proposed Centralized Firewall Management must be capable of supporting RAID with at least 16TB usable capacity.

3.1.6. The proposed Centralized Firewall Management must be have redundant power supply.

3.2. Please see additional feature specifications on **ANNEX "A".**

B. FIELD OFFICES (FO) REQUIREMENT

1. Next Generation Unified Threat Management Device for Field Offices

1.1. Functional Requirements

Platform

1.1.1. The Service Provider shall propose SEVENTEEN (16) 10G Next Generation Firewalls (proposed firewalls) with one (1) spare with a capability of supporting at least TWO (2) gigabit per second of application firewall throughput and at least SEVEN HUNDRED FIFTY (750) megabit per second for threat prevention and modern malware protection.

1.1.2. The proposed firewalls shall support at least ONE HUNDRED FIFTY-THOUSAND (150,000) concurrent sessions and at least TEN THOUSAND (10,000) new sessions per second.

1.1.3. The proposed firewalls should have at least FOUR (4) gigabit network ports and FOUR (4) 10G network ports inclusive of at least sixteen (16) SFP/SPF+ transceivers that are necessary to establish complete connectivity with existing network devices in the location.

1.1.4. The proposed firewalls must allow policy rule creation for application identification, user identification, threat prevention, Uniform Resource Locator (URL) filtering, traffic management Quality of Service (QoS) per policy and scheduling in a single unified rule and not in multiple data-entry locations in the management console.

1.1.5. The proposed firewalls shall have the hardened Operating System (OS) and built as a firewall appliance (i.e. not on generic server hardware) and shall handle traffic in a single pass stream-based manner with all features turned on. It shall be optimized for layer 7 application level content processing and have special Application-Specific Integrated Circuit (ASIC) to handle signature matching and processing in a single pass parallel processing architecture.

1.1.6. The proposed firewalls shall be administered centrally on the central management appliance using the same brand.

1.1.7. The proposed firewall shall have modern malware protection that identifies unknown malicious files by directly and automatically executing them in a virtual cloud-based environment to expose malicious behavior even if the malware has never been seen in the wild before without the need for additional hardware.

1.1.8. The proposed firewalls must have passed and been certified by third party evaluations (e.g. NSS Labs, ICSA Labs, CSfC, ANSSI).

1.2. Please see additional feature specifications on **ANNEX "A".**

C. DISASTER RECOVERY SITE: REMOTE DATACENTER

1. Next Generation Unified Threat Management Device for DR Site

1.1. Functional Requirements

Platform

1.1.1. The Service Provider shall propose TWO (2) 10G Next Generation Firewalls (inclusive of spare) with a capability of supporting at least FIVE (5) GIGABIT per second of application firewall throughput and at least TWO (2) GIGABIT per second for threat prevention and modern malware protection.

1.1.2. The proposed firewalls shall support at least ONE million (1,000,000) concurrent sessions and at least ONE HUNDRED TWENTY THOUSAND (120,000) new sessions per second.

1.1.3. The proposed firewalls shall support at least FIVE THOUSAND (5,000) concurrent sessions of SSL VPN clients inclusive of any required subscription licenses.

1.1.4. The proposed firewalls should have at least TWENTY (20) 10G network ports inclusive of at least sixteen (16) SFP/SPF+ transceivers that are necessary to establish complete connectivity with existing network devices in the location.

1.1.5. The proposed firewalls must allow policy rule creation for application identification, user identification, threat prevention, Uniform Resource Locator (URL) filtering, traffic management Quality of Service (QoS) per policy and scheduling in a single unified rule and not in multiple data-entry locations in the management console.

1.1.6. The proposed firewalls shall have the hardened Operating System (OS) and built as a firewall appliance (i.e. not on generic server hardware) and shall handle traffic in a single pass stream-based manner with all features turned on. It shall be optimized for layer 7 application level content processing and have special Application-Specific Integrated Circuit (ASIC) to handle signature matching and processing in a single pass parallel processing architecture.

1.1.7. The proposed firewalls shall be administered centrally similar to the central office and field offices using the central management solution.

1.1.8. The proposed firewall shall have modern malware protection that identifies unknown malicious files by directly and automatically executing them in a virtual cloud-based environment to expose malicious behavior even if the malware has never been seen in the wild before without the need for additional hardware.

1.1.9. The proposed firewalls must have passed and been certified by third party evaluations (e.g. NSS Labs, ICSA Labs, CSfC, ANSSI).

1.1.10. Proposed firewall must be configured with HIGH AVAILIBILITY.

1.2. Please see additional feature specifications on **ANNEX "A".**

II. Next Generation Intrusion Prevention System (IPS) for DSWD

1. Central Office Requirement:

1.1. Sensors:

1.1.1. Appliance with at least 8x 10G ports capable of at least 10Gbps inspection throughput.

1.2. Management Center:

1.2.1. Appliance purposely built for management of IPS Sensors describe above.

1.3. Please see additional feature specifications on **ANNEX "B".**

2. Remote Datacenter Requirement:

2.1. Sensors:

2.1.1. Appliance with at least 10x5 in-line pairs 10G ports capable of 10Gbps inspection throughput.

2.1.2. Must connect to the Management System located at Central Office.

2.2. Please see additional feature specifications on **ANNEX "B".**

III. Project Coverage

A. Service Area

The **service provider** will be reporting to the DSWD offices if there are major issues or concerns that needs resolution.

1. Central Office - DSWD Complex, Batasan Hills, Quezon City

2. DR Site – Clark Pampanga (whichever is the active DR Site of DSWD for the year)

3. 16 Field Offices

Field Office	Site
1. DSWD Field Office 1	San Fernando City, LaUnion
2. DSWD Field Office 2	Carig Sur, Tuguegarao
3. DSWD Field Office 3	San Fernando City, Pampanga
4. DSWD Field Office 4A	Muntinlupa City
5. DSWD Field Office 4B	Malate, Manila
6. DSWD Field Office 5	Legaspi City, Albay
7. DSWD Field Office 6	Molo, Iloilo
8. DSWD Field Office 7	Cebu
9. DSWD Field Office 8	Tacloban City, Leyte
10.DSWD Field Office 9	Zamboanga Del Sur
11.DSWD Field Office 10	Misamis Oriental, CDO
12.DSWD Field Office 11	Davao del Sur
13.DSWD Field Office 12	Koronadal City, South Cotabato
14.DSWD Field Office CARAGA	Butuan City, Agusan del Norte
15.DSWD Field	Baguio City, Benguet

Office CAR	
16.DSWD Field Office NCR	Legarda, Manila

B. Service Coverage

1. Response On-site (24x7, 4 Hours Onsite)

On-site response time is 24x7x4 for all DSWD sites within Metro Manila. All FO's outside metro manila will be on next available flight. Secure remote access can also be initiated to check and may address all related firewall concerns.

1.1. Resolution Time

The resolution time varies depending on the complexity of the problem reported.

	Business Critical (Fatal - High)	Business Critical (Medium - Impaired)	Non-Business Critical (Low - information)
Number of Hours	0 - 4 hours	0 – 8 hours	1-3 days

1.2. Definition of Terms

1.2.1. Fatal High - Service is down, total system inoperability.

1.2.2. Medium Impaired - Partial System inoperability.

1.2.3. Low Information - Minor system update, patches, business services is up.

1.3. Escalation (24x7)

1.3.1. For technical support or assistance required, the service provider should put in the contract numbers and other contract information.

Level	Hour Lapsed	Contact Person	Contact Number	Position

I	Initial call within 30 mins			
II	> 4 hours			
III	> 8 hours			

2. **Hardware/ Software Support**

Since this is a manage service project, all the hardware and accessories are part of the service provider's property. A spare should be provided for the unit as quick replacement in the event of hardware fault.

A transition support should likewise be provided for at least three (3) months right after the contract period to prevent prolonged service interruption on the part of the Department while the successor services is being implemented.

3. **Scope of Responsibility**

The scope of work covers the following:

3.1. Supply and delivery of Next Generation Firewall devices.

3.2. Supply and delivery of Next Generation IPS devices.

3.3. Administration and management of firewall in the perimeter gateway on all 18 sites.

3.4. Maintain, configure, troubleshoot and address all security concerns in the perimeter gateway.

3.5. Setup and configuration of DSWD security policy.

3.6. Proactive monitoring of any security breach on the perimeter and update / resolve security issues.

3.7. Analysis and presentation of log reports and security events.

4. **Capacity Building and Technology Transfer**

4.1. Provide specialized training of Next Generation Perimeter Devices for at least two (2) Central Administrators.

4.2. Provide specialized Training/ Certification on Intrusion Prevention/ Basic Hacking Countermeasures for at least 25 support engineers from Central and Field Offices.

5. **Network Diagram:** Please see **ANNEX "C".**

IV. Project Requirement

1. The service provider/ supplier must deploy and configures all devices and updates on an optimal setting, based on industry's best practices.
2. The service provider must have been in the business for at least 10 years.
3. The service provider must have at least 5 years experience and expertise in providing professional services such as managed service, maintenance support, on-call troubleshooting, consulting, training and migration services.
4. The solution offered must have been in the market for at least 5 years.
5. The service provider must have previously deployed successfully at least once each in Luzon, Visayas, Mindanao and the NCR.
6. The service provider must allow a transition period of at least 3 months beyond the last contract month to prevent service interruption while successor project is being implemented.
7. The service provider must have deployed at a simila project having an SLCC of at least 40% of the approved budget ceiling.

ANNEX "A"

1. **ADDITIONAL SPECIFICATIONS FOR NEXT GENERATION FIREWALLS**

A. Functional Requirements

1. **Operational Mode**

1.1. The proposed firewalls shall support policy based Network Address Translation (NAT) and Port Address Translation (PAT) and able to operate in routing/NAT mode.

1.2. The proposed firewalls shall support Denial of Service (DoS) and fragmented packet Transmission Control Protocol (TCP) reassembly, brute force attack, “SYN cookie”, “IP spoofing” and malformed packet protection.

1.3. The proposed firewalls shall support transparent and tap mode within the appliance.

1.4. The proposed firewalls shall support 802.1Q Virtual Local Area Networks (VLANs) tagging (in tap, transparent, layer 2 and layer 3).

1.5. The proposed firewalls shall support dual IPv4 and IPv6 stacks application control and threat inspection support in tap mode, transparent mode, layer 2 and layer 3.

1.6. The proposed firewalls shall support standards based link aggregation (IEEE 802.3ad) to achieve higher bandwidth.

1.7. The proposed firewalls shall support logical Ethernet sub-interfaces tagged and untagged.

1.8. The proposed firewalls shall support static, Routing Information Protocol version 2 (RIPv2), Open Shortest Path First (OSPF) and Border Gateway Protocol version 4 (BGPv4) routing protocols.

1.9. The proposed firewalls shall support the ability to circumvent the route lookup process and the subsequent Policy-Based Forwarding (PBF) lookup for return traffic (server to client). The firewalls shall use the original incoming interface as the egress interface. However, if the source IP is in the same subnet as the incoming interface on the firewalls, symmetric return shall not take effect.

1.10. The proposed firewalls shall support policy based forwarding based on zone, source or destination address, source or destination port, application and Active Directory (AD)/ Lightweight Directory Access Protocol (LDAP) Remote Authentication Dial In User Service (RADIUS) user or user groups.

1.11. The proposed firewalls shall support Domain Name System (DNS) proxy and Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay.

1.12. The proposed firewalls shall support IPv6 routing for virtual routers.

2. **Firewalls Management**

2.1. The proposed firewalls solution shall be managed from Web-based Graphical User Interface (GUI) and Command-Line Interface (CLI).

2.2. The proposed firewalls shall be able to manage itself without the need for external servers or appliances, at the same time with an option to be managed centrally.

2.3. The proposed firewalls shall have a dedicated management port that has separate routing tables from the other production interfaces.

2.4. The proposed firewalls management shall be able to granularly assigned management functions for each management user group or for individual user.

2.5. The proposed the firewalls is able to schedule log exports using SCP or FTP protocol.

2.6. The proposed firewalls shall have a reporting management system capable of generating reports on a manual ad-hoc or schedule (daily, weekly, monthly, etc) basis.

2.7. The proposed firewalls shall be able to generate reports on individual user ID with (but not limited to) the following activities, Application Usage, accessed websites & URL Categories.

3. **Policy Based Controls**

The proposed firewall shall support:

3.1. Policy control by port and/ or protocol.

3.2. Policy control based on application or application category.

3.3. Policy control based on user or user group.

3.4. Policy control based on IP address.

3.5. Policy control by country code.

3.6. Per policy Secure Shell (SSH) decryption and inspection.

3.7. IPv6 rules/ objects.

3.8. Multicast rules/ objects.

4. **Application Security Policy**

4.1. The proposed firewalls shall support network traffic classification, which identifies applications across all ports irrespective of port/protocol/evasive tactics.

4.2. The proposed firewalls shall have multiple mechanisms for classifying applications and application identification technology based upon Intrusion Prevention System (IPS) or deep packet inspection.

4.3. The proposed firewalls shall provide the ability to allow the organization to write its own customized of application identification signature for new application not in the current application database or for any in-house applications.

4.4. The proposed firewalls shall include a searchable list of currently identified applications with explanation and links to external sites for further clarification.

4.5. The proposed firewalls shall allow dynamic

updates of the application database (DB) and not require a service restart or reboot. 4.6. The proposed firewalls shall warn the end-user with a customizable page when the application is blocked. 4.7. The proposed firewalls shall support user-identification allowing AD, LDAP, RADIUS groups, or users to access a particular application, while denying others. 5. **URL Filtering** 5.1. The proposed firewalls shall support URL filtering/ categorization and have database stored locally on the appliance. 5.2. The proposed firewalls shall support logs populated with end user activity reports for site monitoring within the local firewalls. 5.3. The proposed firewalls shall support URL filtering policies by AD/ LDAP user, user group, machines and IP address/ range. 6. **Threat Prevention** 6.1. The proposed firewalls shall support IPS features on the proposed firewalls appliance and antivirus and anti-spyware. 6.2. The proposed firewalls shall perform stream based antivirus and anti-spyware and not store-and-forward traffic inspection. 6.3. The proposed firewalls shall block known network and application-layer vulnerability exploits. 7. **Data Filtering** 7.1. The proposed firewalls shall support file identification by signature and not file extensions. 7.2. The proposed firewalls shall unpack zipped file for packet inspection.	

8. **User Identification**

8.1. The proposed firewalls shall support authentication services for AD, LDAP, eDirectory, RADIUS, Kerberos and client certificate.

8.2. The proposed firewalls shall support the creation of security policy based on AD Users and Groups in addition to source/destination IP.

8.3. The proposed firewalls shall support user identification in policy without installing an agent on individual endpoints.

8.4. The proposed firewalls shall populate and correlate all logs with user identity (traffic, IPS, URL, data, etc) without any additional products or modules in real-time.

9. **SSL/ SSH Decryption**

9.1. The proposed firewalls shall be able to identify, decrypt and evaluate SSL/SSH traffic in an outbound and inbound connection.

9.2. The proposed firewalls shall be able to block SSL sessions with expired server certs.

9.3. The proposed firewalls shall be able to block SSL sessions with untrusted server certs.

9.4. The proposed firewalls shall be able to restrict certificate extensions to limit the purposes for which the generated certificate will be used.

9.5. The proposed firewalls shall be able to block SSL and SSH sessions for unsupported modes (version, cipher suites).

9.6. The proposed firewalls shall be able to decrypt in tap, transparent, layer 2 and layer 3 modes.

10. **Modern Malware Prevention**

10.1 The proposed firewalls are able to provide detection for unknown Malware by using sandboxing technology. Furthermore, it is able to support automatic creation of signatures to detect the unknown malware within 24-hours after detection.

10.2 The proposed firewall is able to provide an on-box reporting of the unknown Malware i.e. replication behavior, command-and-control server info, file downloading, etc.

10.3 When an unknown malware is detected, the proposed firewalls are able to provide the option of prompting the user (via a customized web page) as well as allowing the user to decide whether to upload or download the suspected malicious content.

10.4 The proposed firewalls shall support in-line control of malware infection and command/control traffic.

10.5 The proposed firewalls shall support DNS-based signatures to detect specific DNS lookups for hostnames that have been associated with malware.

11. **Client Remote Access**

11.1. The proposed firewalls shall allow remote users to access the internal corporate network by automatically establishing either an SSL or IPSec-based VPN connection depending on location and configuration.

11.2. The proposed firewalls shall provide Remote Access agent that supports various Client Platforms i.e. Mac OSX, Windows 7, etc..

11.3. The proposed firewalls remote access agent shall be provide host information profile (i.e. patch level of OS, status of Anti-Virus software or Host-based IPS, etc.) to the firewalls to ascertain whether the host meets the required security requirement before allowing access into the internal corporate network.

11.4. The proposed firewalls remote access agent shall be able to determine whether the client is within the internal corporate network. If its not, it shall be able to automatically connect to the firewalls and establish a secure tunnel (via SSL or IPSec VPN).

11.5. The proposed firewalls shall be able to authenticate remote users via AD, LDAP, eDirectory, RADIUS, Kerberos and client certificate.

12. **Internet Protocol Version 6 (IPv6) Requirement**

12.1 The Tenderer shall furnish/design the firewalls appliance (also known as 'Infrastructure' to support the co-existence of IPv4 and IPv6. If it is not compliant, the Tenderer shall advise the roadmap and propose how the system can be upgraded.

13. **Connectivity**

13.1. The propose the Next Generation Firewalls Appliance that will support operations in the following scenarios, but not limited to:

13.1.1. Connect to legacy network and application, which supports IPv4 only.

13.1.2. Connect to local Internet Service Provider (ISP) and IPv6 service and the end-user using IPv6 only.

13.1.3. Connect to local ISP and IPv4 service and the remote ISP and IPv6 service, and the remote end-user using IPv6 only.

13.2. The proposed firewalls shall support the following IPv6 features, but not limited to:

13.2.1. Able to support Network Address Translation from IPv6 to IPv4.

13.2.2. Able to support Stateless Address Auto-Configuration (SLAAC) for IPv6-configured interfaces. The proposed firewalls shall be able to send router advertisement (RA) messages on connected links in order to inform hosts of the IPv6 prefixes that they can use for address configuration.

13.2.3. Able to support routing of IPv6 traffic over an IPSec tunnel established between IPv4 endpoints.

13.2.4. Able to provide IPv6 connectivity for firewalls administrative controls (i.e. Syslog, SNMP, DNS, NTP, Admin Authentication Sources, etc.).

14. **Maintenance and Support**

14.1. The Tenderer shall provide information on whether any patches, upgrades or additional hardware and/or software and/or services are needed to be purchased or installed in order for the proposed hardware and software to support the co-existence of IPv4 and IPv6 environment.

2. **ADDITIONAL SPECIFICATIONS FOR A CENTRALIZED FIREWALL MANAGEMENT SYSTEM**

2.1. Central Visibility and Global Policy Control

2.1.1. Graphical view of applications, URL, threat and data traversing all firewalls

2.1.1.1. Capable of displaying summary of applications running on the network, the users and the security impact;

2.1.1.2. Nationwide Admin will have the capabilities to manage all Next Gen Firewalls deployed at any remote site of DSWD. Same access with the local admin; and,

2.1.1.3. Nationwide admin can create and enforce policies/templates on any individual devices or all devices.

2.1.2. Can control application enablement, QoS, URL filtering and other policies across nationwide network of DSWD

2.2. Traffic Monitoring and reporting for Analysis and Forensic

2.2.1. Traffic monitoring and reporting tools available both local and National (whole DSWD nationwide network);

2.2.2. Access to all Logs (log viewer), either local, individual or all devices;

2.2.3. Custom Reporting: both predefined and customized / grouped reports can be done;

2.2.4. User activity Reports: aggregate and individual device/users can be created; and,

2.2.5. Log forwarding: aggregated reports from all devices in the nationwide network of DSWD can be created.

2.3. Number of Devices Supported for centralized Management. It must support all remote sites of DSWD with the Next Generation firewall: **At least 25 devices.**

2.4. High Availability Support: must be capable of Active/Passive modes.

2.5. Admin Authentication: must be capable of Local and Radius databases.

2.6. Management Tools and APIs: GUI, Command Line and XML-based REST API.

2.7. Storage: at least 16TB with RAID storage.

2.8. Rack Mount: can be deployed on a rack.

ANNEX "B"

1. ADDITIONAL FEATURE SPECIFICATIONS FOR NEXT GENERATION INTRUSION PREVENTION SYSTEMS (IPS) FOR DSWD

1.1. Advanced Threat Protection

1.1.1. The proposed solution must have at least TEN (10) gigabits per second throughput while having application visibility control and intrusion prevention active.

1.1.2. The proposed solution platforms must be based on a hardened operating system.

1.1.3. The detection engine must be capable of operating in both passive (i.e., monitoring) and inline (i.e., blocking) modes.

1.1.4. The detection engine should support Layer 2 deployment so that it provides packet switching and inspection between two or more network segments.

1.1.5. The detection engine should support Layer 3 deployment where it can route and inspect traffic between two or more interfaces.

1.1.6. Detection rules must be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.

1.1.7. Detection rules provided by the vendor must be documented, with full descriptions of the identity, nature, and severity of the associated vulnerabilities and threats being protected against.

1.1.8. The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.).

1.1.9. The detection engine must be capable of detecting variants of known threats, as well as new threats (i.e., so-called "unknown threats").

1.1.10. The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported.

1.1.11. The detection engine must inspect not only Network Layer details and information resident in packet headers,

but a broad range of protocols across all layers of the computing stack and packet payloads as well. 1.1.12. The detection engine must be resistant to various URL obfuscation techniques common to HTML-based attacks. 1.1.13. The solution must incorporate measures to minimize the occurrence of both false positives and false negatives (i.e., mistaken and missed detection events, respectively). 1.1.14. The solution must be capable of detecting multi-part or extended threats by aggregating and correlating the multiple, disparate events associated with them. 1.1.15. The detection engine must be capable of inspecting traffic associated with different network segments differently (as opposed to having only one policy per interface). 1.1.16. Sensors must be capable of performing packet-level forensics and capturing raw packet data in response to individual events without significant performance degradation. 1.1.17. The detection engine must support multiple options for directly responding to events, such as monitor only, block offending traffic, replace packet payload, and capture packets. 1.1.18. The management platform must be capable of setting thresholds such that multiple instances of specific events are required before an alert is issued. 1.1.19. The solution must be capable of detecting and blocking IPv6 attacks. 1.1.20. The solution must provide IP reputation feed that comprised of several regularly updated collections of IP addresses determined by the proposed security vendor to have a poor reputation.	

1.1.21. The solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.

1.1.22. The solution must have the option of providing network-based detection of malware by checking the disposition of known files in the cloud using the SHA-256 file-hash as they transit the network (SHA-256 and target IP address should be given to aid remediation efforts).

1.1.23. The solution must have a network file trajectory feature that can provide a visual, interactive representation of the path an infected file takes across the network, to help us understand the broader impact, context, and spread of malware across the network and endpoints. This view depicts point of entry, propagation, protocols used, and the users or endpoints involved in the transfer.

1.1.24. The solution must support geolocation lookup.

1.2. Real-Time Contextual Awareness

1.2.1. The solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.

1.2.2. The solution must be capable of passively gathering information about session flows for all monitored hosts, including start/end time, ports, services, and amount of data.

1.2.3. The solution must be capable of passively detecting pre-defined services, such as FTP, HTTP, POP3, Telnet, etc., as well as custom services.

1.2.4. The solution must be capable of storing user-defined host attributes, such as host criticality or administrator contact information, to assist with compliance monitoring.

1.2.5. The solution must be capable of passively gathering user identity information, mapping IP addresses to username, and making this information available for event management purposes.

1.2.6. The solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.

1.2.7. The solution must be capable of identifying “Jailbroken” mobile devices, which can help to enforce mobile device usage policies on the network.

1.2.8. The solution must provide a detailed, interactive graphical summary that includes data on applications, application statistics, connections, intrusions events, hosts, servers, users, file-types, malwares and relevant URLs. These data should be presented in the form of vivid line, bar, pie and donut graphs accompanied by detailed lists (Administrator should easily create and apply custom filters to fine-tune the analysis).

1.2.9. The aforementioned network and user intelligence must be passively gathered using existing IPS devices (no separate hardware required).

1.3. Intelligent Security Automation

1.3.1. The solution must be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behavior of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events.

1.3.2. The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward.

1.3.3. The solution must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.

1.3.4. The solution must be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.

1.3.5. The solution must be capable of defending against IPS-evasion attacks by automatically using the most appropriate defragmentation and stream reassembly routines for all traffic based on the characteristics of each destination host.

1.4. Control Compliance

1.4.1. The solution must have the option for integrating application control to reduce risks associated with applications usage and client-side attacks. It should provide a means of enforcing acceptable use policies of up to 2000 application detectors.

1.4.2. The solution must support creation of user-defined application protocol detectors.

1.4.3. The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions:

- Protocols: HTTP, SMTP, IMAP, POP;
- Direction: Upload, Download, Both; and,
- File Types: Office Documents, Archive, Multimedia, Executable, PDF, Encoded, Graphics, and System Files.

1.4.4. The proposed solution should provide an option to include URL filtering for enforcing Internet content filtering so as to reduce web born threats and improve productivity.

Each URL in the data set must has an associated category and reputation. URL category is a general classification for the URL while URL reputation represents how likely the URL is to be used for purposes that might be against the organization's security policy.

1.4.5. The solution must provide capabilities for establishing and enforcing host compliance policies and alerting on violations.

1.4.6. The solution must be capable of exempting specific hosts from specific compliance rules and suppressing corresponding compliance events and alerts.

1.4.7. The solution must be capable of easily identifying all hosts that exhibit a specific attribute or non-compliance condition.

1.5. Network Behavior Analysis (NBA)

1.5.1. The solution must provide a full-featured NBA capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter IPS). This includes the ability to establish "normal" traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.

1.5.2. The NBA capability must provide visibility into how network bandwidth is consumed to aid in troubleshooting network outages and performance degradations.

1.5.3. The NBA capability must provide the ability to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.

1.5.4. The NBA capability must provide the option of supplying endpoint intelligence to the IPS for correlation against intrusion events to aid in event impact prioritization.

1.5.5. The same network devices used for IPS must also be used as part of the NBA capability. No NBA-only device should be required.

1.5.6. The same management platform used for IPS must also be used to manage the NBA capability. No NBA-only management components should be required.

1.6. Management and Usability

1.6.1. The management platform must be capable of centralized, life cycle management for all sensors.

1.6.2. The management platform must be delivered in virtual appliance form factor (management system and UI must provide the same features and functions as in the physical appliance).

1.6.3. The management platform must be capable of aggregating IDS/IPS events and centralized, real-time monitoring and forensic analysis of detected events.

1.6.4. The management platform must be accessible via a web-based interface and ideally with no need for additional client software.

1.6.5. The management platform must provide a highly customizable dashboard.

1.6.6. The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows.

1.6.7. The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.

1.6.8. The management platform must include a scheduling subsystem to facilitate automation of routine tasks, such as backups, upgrades, report creation, and policy application.

1.6.9. The management platform must include one or more default (i.e., pre-defined) detection policy configurations to help simplify initial deployment.

1.6.10. The management platform must be capable of grouping both sensors and policies to help simplify configuration management.

1.6.11. The management platform must provide the capability to easily view, enable, disable, and modify individual rules, as well as groups or categories of rules.

1.6.12. The management platform must be capable of automatically receiving rule updates published by the vendor and automatically distributing and applying those rule updates to sensors.

1.6.13. The management platform must be capable of backup and rollback for sensor configurations and the management platform itself.

1.6.14. The management platform must include flexible workflow capabilities for managing the complete life cycle of an event, from initial notification through to any response and resolution activities that might be required.

1.6.15. The management platform must provide the ability to view the corresponding detection rule for each detected event, along with the specific packet(s) that caused it to be triggered.

1.6.16. The management platform must support both internal and external databases/systems for storage of event data, logs, and other system-generated information.

1.6.17. The management platform must be capable of synchronizing time between all components of the system via NTP.

1.6.18. The management platform must be capable of logging all administrator activities, both locally and to a remote log server.

1.6.19. The solution must support LDAP for single sign-on to sensors and the management console.

1.7. Reporting and Alerting

1.7.1. The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.

1.7.2. The management platform must allow quick report customization by importing from dashboards, workflows and statistics summaries.

1.7.3. The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.

1.7.4. The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).

1.8. Reliability and Availability

1.8.1. Sensors must support built-in capability of failing open, such that communications traffic is still allowed to pass if the inline sensor goes down.

1.8.2. The product must support "Lights Out Management" capability where remote upgrade, restore, and downgrade functionality without physical access to the appliance being required.

1.8.3. The sensor platforms must support a range of models, including modular design on the high-end and standard connectivity options on the low-end. The high-end sensor platforms must be capable of offering additional flexibility through stacking to increase throughput as your inspection needs grow without using external load balancing solutions.

1.8.4. The management platform must be capable of monitoring the health of all components and issuing alerts for anomalous conditions.

1.8.5. Intra-system communications must be secure.

1.8.6. The supplier must have a detailed process for customer submission of product-related faults and the resolution of those faults, including provisions for escalation of critical or unresolved issues.

1.9. Third-Party Integration

1.9.1. The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable automatic response to threats by external components and remediation applications, such as routers, firewalls, patch management systems, etc.

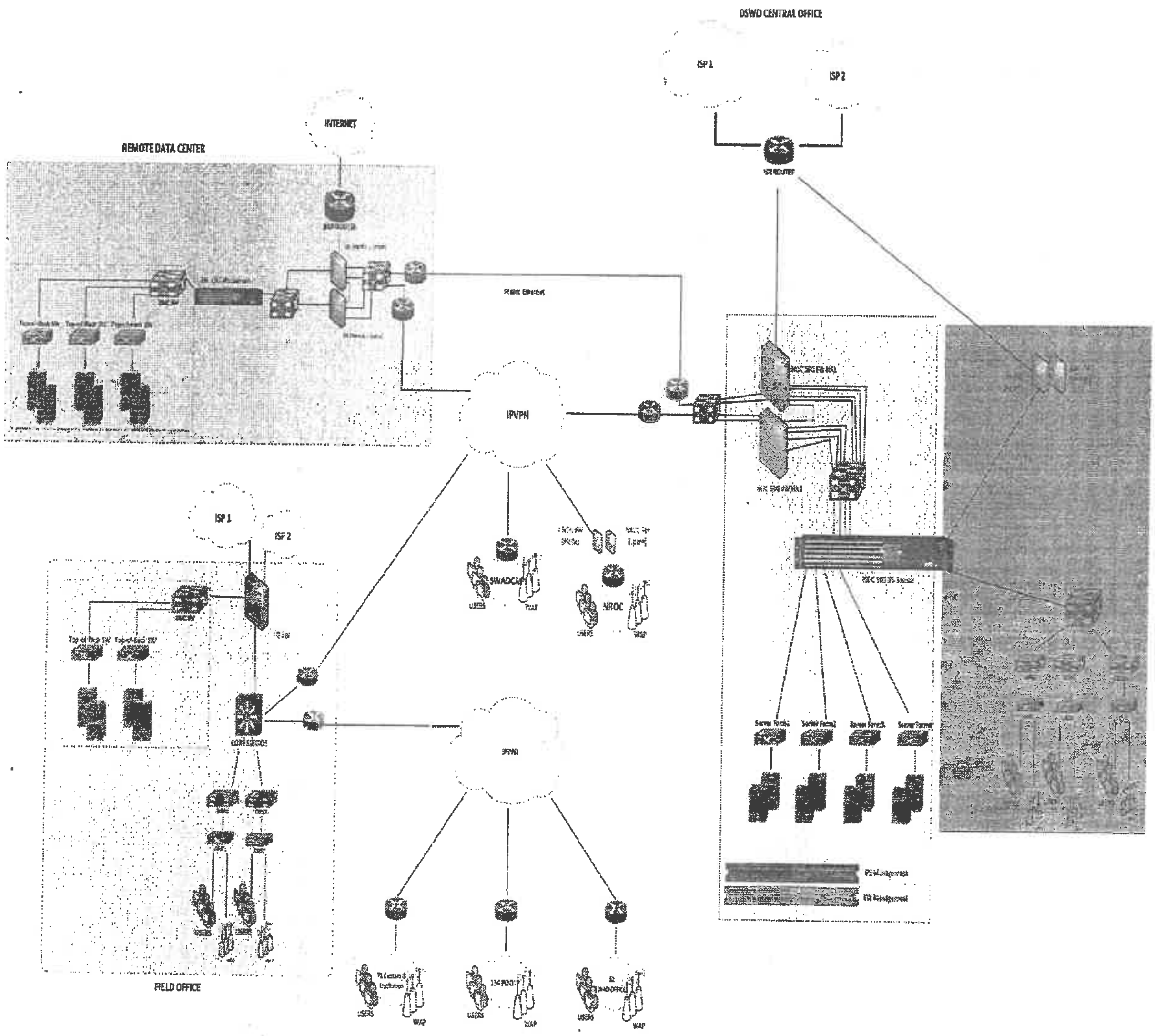
1.9.2. The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as trouble-ticketing systems, Security Information and Event Managers (SIEMs), systems management platforms, and log management tools.

1.9.3. The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to receive information from external sources, such as configuration management databases, vulnerability management tools, and patch management systems, for threat correlation and IT policy compliance purposes.

1.9.4. The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to export SNMP information to

network management systems. 1.9.5. The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to obtain network intelligence (i.e., NetFlow) from Cisco routers and switches. **1.10. Industry Recognition** 1.10.1. The proposed vendor must have a track record of continuous improvement in threat detection and must have successfully completed the latest NSS Labs' IPS Methodology testing with a minimum attacks blocking rate of 97% and correctly identified 100% of evasion attempts without error.	

DSWD ENTERPRISE NETWORK ARCHITECTURE



Name of Bidder: ______________________________

Name of Authorized Representative: ______________________________

Signature of Authorized Representative: ______________________________

Date: ____________________

PRE-BID CONFERENCE

SUBSCRIPTION OF MANAGED SERVICES FOR A COMPLETE SUITE OF PRIMARY ICT SECURITY DEVICES

(ITB NO. GOP/20-DSWD-017)

03 January 2020 at 03:00 PM

OUS-DRMG, Room 202, Directors Dormitory, DSWD Central Office, IBP Road, Batasan Hills, Quezon City

ATTENDANCE SHEET

NO.	NAME	OFFICE	SEX	EMAIL	CONTACT NO.	SIGNATURE
1	USec. Felicisimo C. Budiongan (BAC Chairperson)	OUSDRMG	M	fcbudiongan@dswd.gov.ph		
2	USec. Rene Glen O. Paje (BAC Regular Member)	OUSISP	M	rgopaje@dswd.gov.ph		
3	ASec. Noel M. Macalalad (BAC Alternate Member)	OASSCB	M	nmmacalalad@dswd.gov.ph		
4	Dir. Ernestina Z. Solloso (BAC Regular Member)	4Ps	F	ezsolloso@dswd.gov.ph		
5	Dir. Irene B. Dumlao (BAC Alternate Member)	SMS	F	ibdumlao@dswd.gov.ph		
6	Dir. Emmanuel P. Privado (BAC Regular Member)	NRLMB	M	epprivado@dswd.gov.ph		
7	Mr. Felix M. Armeña (BAC Alternate Member)	ICTMS	M	fmarmena@dswd.gov.ph		
8	Dir. Andrew J. Ambubuyog (BAC Provisional Member)	ICTMS	M	ajambubuyog@dswd.gov.ph		
9	Atty. Karina Antonette A. Agudo	PMS	F	kaagudo@dswd.gov.ph	Loc. 121 -124	
10	Ms. Oliva C. Arcaina	BAC Secretariat	F	ocarcaina@dswd.gov.ph	Loc. 121 -124	
11	Mr. Ramon M. Villareal Jr.	BAC Secretariat	M	rmvillarealjr@dswd.gov.ph	Loc. 121 -124	
12	Mr. William V. Garcia Jr.	BAC Secretariat	M	wvgarciajr@dswd.gov.ph	Loc. 121 -124	
13	Ms. Katrina E. Garcia	BAC Secretariat	F	kegarcia@dswd.gov.ph	Loc. 121 -124	

ATTENDANCE SHEET

NO.	NAME	OFFICE	SEX	EMAIL	CONTACT NO.	SIGNATURE
14	Mr. Arjay C. Dimafelix	BAC Secretariat	M	acdimafelix@dswd.gov.ph	Loc. 121 -124	
15	Mr. Ramises B. Esteban	BAC Secretariat	M	rbesteban@dswd.gov.ph	Loc. 121 -124	
16	Ms. Luzvi S. Dabuet	BAC Secretariat	F	lsdabuet@dswd.gov.ph	Loc. 121 -124	
17	Ms. Danilyn A. Dedeles	BAC Secretariat	F	dadedeles@dswd.gov.ph	Loc. 121 -124	
18	Ms. Marden D. Aquino	BAC Secretariat	F	mdaquino@dswd.gov.ph	Loc. 121 -124	Mdaquino
19	Mr. Glenn Patrick A. Leynes	BAC Secretariat	M	gpaleynes@dswd.gov.ph	Loc. 121 -124	
20	Mr. Prince A. Lee	BAC Secretariat	M	palee@dswd.gov.ph	Loc. 121 -124	
21	Ms. Filipinas B. Alfonso	BAC Secretariat	F	fbalfonso@dswd.gov.ph	Loc. 121 -124	
22	Mr. Lourence C. Buenaventura	BAC Secretariat	M	lcbuenaventure@dswd.gov.ph	Loc. 121 -124	
23	Joshua Kevin Jovellanos	FMS-CMD	M			
24	Roy Ocampo	ICTMS	M			
25	Jeson Diaz	ICTMS	M			
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
37						
38						
39						
40						

PRE-BID CONFERENCE

SUBSCRIPTION OF MANAGED SERVICES FOR A COMPLETE SUITE OF PRIMARY ICT SECURITY DEVICES

(ITB NO. GOP/20-DSWD-017)

03 January 2020 at 03:00 PM

OUS-DRMG, Room 202, Directors Dormitory, DSWD Central Office, IBP Road, Batasan Hills, Quezon City

BIDDERS ATTENDANCE SHEET

NO.	NAME	OFFICE	SEX	EMAIL	CONTACT NO.	SIGNATURE
1	Chris Garcia	AMTI	M	christopher.garcia@amti.com.ph	09178548926	
2	Ryelan Bautista	AMTI	M	ryelan.bautista@amti.com.ph	0917159620	
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						